IN THE CLAIMS

1. (currently amended) A security system reader comprising:

a transceiver that transmits a stimulus signal and that receives a signal containing an authentication code; and,

a processor that determines whether the received authentication code is from a badge or a fingerprint keyfob, and that performs an authentication of the authentication code dependent upon whether the authentication code is from the badge or from the fingerprint ~~keybob~~ keyfob.

2. (original) The security system reader of claim 1 wherein the authentication code from the fingerprint keyfob comprises a fingerprint signature and an identifier, and wherein the processor is arranged to perform an authentication of the authentication code based upon both the fingerprint signature and the identifier in the authentication code from the fingerprint keyfob.

3. (original) The security system reader of claim 2 wherein the identifier in the authentication code

from the fingerprint keyfob comprises a rolling identifier.

4. (original) The security system reader of claim 2 wherein the fingerprint signature comprises a digitized fingerprint signature.

5. (original) The security system reader of claim 2 wherein the processor compares the fingerprint signature to fingerprint signatures in a list of fingerprint signatures and also compares the identifier in the authentication code from the fingerprint keyfob to an identifier maintained by the processor.

6. (original) The security system reader of claim 5 wherein the identifier in the authentication code from the fingerprint keyfob comprises a rolling identifier, and wherein the processor compares the rolling identifier in the authentication code from the fingerprint keyfob to a rolling identifier maintained by the processor.

7. (currently amended) A method of providing access comprising:

receiving a signal containing an authentication code;

determining whether the authentication code is from a badge or a fingerprint keyfob;

determining whether the authentication code is authentic dependent upon whether the authentication code is from the badge or from the fingerprint ~~keybob~~ keyfob; and,

if the authentication code is authentic, permitting access.

8. (original) The method of claim 7 wherein the authentication code from the fingerprint keyfob comprises a fingerprint signature and an identifier, and wherein the determining of whether the authentication code is authentic comprises determining whether both the fingerprint signature and the identifier in the authentication code from the fingerprint keyfob are authentic.

9. (original) The method of claim 8 wherein the identifier in the authentication code from the fingerprint keyfob comprises a rolling identifier.

10. (original) The method of claim 8 wherein the fingerprint signature comprises a digitized fingerprint signature.

11. (original) The method of claim 8 wherein the determining of whether the authentication code is authentic comprises:

comparing the fingerprint signature to fingerprint signatures in a list of fingerprint signatures; and,

comparing the identifier in the authentication code from the fingerprint keyfob to a separately maintained identifier.

12. (original) The method of claim 11 wherein the identifier in the authentication code from the fingerprint keyfob comprises a rolling identifier, and wherein the comparing of the identifier in the authentication code from the fingerprint keyfob to a separately maintained identifier comprises comparing the rolling identifier in the authentication code from the fingerprint keyfob to a separately generated rolling identifier.

13. (original) The method of claim 7 further comprising transmitting a stimulus signal that causes at least one of the badge and the keyfob to transmit the signal containing the authentication code.

14. (original) A method of providing access comprising:

receiving a signal containing an authentication code;

determining whether the authentication code is from a badge or a keyfob;

determining whether the authentication code is authentic; and,

if the authentication code is authentic, permitting access.

15. (original) The method of claim 14 further comprising transmitting a stimulus signal that causes at least one of the badge and the keyfob to transmit the signal containing the authentication code.

16. (original) The method of claim 14 wherein the authentication code from the keyfob comprises first and second portions, wherein the first and second

portions are different types of codes, and wherein the determining of whether the authentication code is authentic comprises determining whether both the first and second portions are authentic.

17. (original) The method of claim 16 wherein the first portion comprises a rolling identifier.

18. (original) The method of claim 16 wherein the determining of whether the authentication code is authentic comprises:

comparing the first portion to a list; and,

comparing the second portion to a separately maintained code.

19. (original) The method of claim 18 wherein the second portion comprises a rolling identifier, and wherein the comparing of the second portion to a separately maintained code comprises comparing the rolling identifier to a separately generated rolling identifier.

20. (original) The method of claim 14 wherein the authentication code from the keyfob comprises a

fingerprint signature and an identifier, and wherein the determining of whether the authentication code is authentic comprises determining whether both the fingerprint signature and the identifier are authentic.

21. (original) The method of claim 20 wherein the identifier in the authentication code from the keyfob comprises a rolling identifier.

22. (original) The method of claim 20 wherein the fingerprint signature comprises a digitized the fingerprint signature.

23. (original) The method of claim 20 wherein the determining of whether the authentication code is authentic comprises:

comparing the fingerprint signature to fingerprint signatures in a list of fingerprint signatures; and,

comparing the identifier in the authentication code from the keyfob to a separately maintained identifier.

24. (original) The method of claim 23 wherein the identifier in the authentication code from the keyfob comprises a rolling identifier, and wherein the comparing of the identifier in the authentication code from the keyfob to a separately maintained identifier comprises comparing the rolling identifier to a separately generated rolling identifier.

25. (new) The method of claim 17 wherein the determining of whether the authentication code is from a badge or a keyfob comprises determining whether the authentication code is from a badge or a fingerprint keyfob.

26. (new) A method of providing access comprising:

receiving a signal containing an authentication code;

determining whether the authentication code is of a first type or of a second different type;

processing the authentication code in a first manner if the authentication code is of the first type and processing the authentication code in a second different manner if the authentication code is of the

second different type to determine whether the authentication code is authentic; and,

if the authentication code is authentic, permitting access.

27. (new) The method of claim 26 wherein the determining of whether the authentication code is of a first type or of a second different type comprises determining whether the authentication code comprises a pre-stored authentication code.

28. (new) The method of claim 26 wherein the determining of whether the authentication code is of a first type or of a second different type comprises determining whether the authentication code is an authentication code derived from a physical characteristic of a human user.

29. (new) The method of claim 28 wherein the determining of whether the authentication code is an authentication code derived from a physical characteristic of a human user comprises determining whether the authentication code is an authentication code derived from a fingerprint of a human user.

30. (new) The method of claim 26 wherein the determining of whether the authentication code is of a first type or of a second different type comprises determining whether the authentication code is a pre-stored authentication code or an authentication code derived from a physical characteristic of a human user.

31. (new) The method of claim 30 wherein the determining of whether the authentication code is an authentication code derived from a physical characteristic of a human user comprises determining whether the authentication code is an authentication code derived from a fingerprint of a human user.